

Module 2 : Gouvernance, gestion des risques et conformité



École / Prépa
ENSEIRB-
MATMECA

En bref

- **Langue(s) d'enseignement:** Français
- **Ouvert aux étudiants en échange:** Non

Présentation

Code interne : EC9IT312

Objectifs

Maîtriser les concepts de la GRC, basés sur les normes, méthodologies et réglementations.

Heures d'enseignement

CI	Cours Intégrés	24h
----	----------------	-----

Syllabus

ISO 27001 et 27002, SMSI, NIS, LPM, EBIOS, etc.

Informations complémentaires

Gouvernance, gestion des risques et conformité

Compétences visées

Ce module appartient au bloc de compétence de l'**Activité 1 (A1) : Gouvernance et gestion des risques en cybersécurité**.

Tâche 1 (A1T1) : Élaborer et piloter la stratégie de gouvernance de la cybersécurité

- A1T1C1 : Définir une politique de sécurité des systèmes d'information (PSSI) alignée sur les normes et réglementations (ISO 27001, RGPD, NIS2).
- A1T1C2 : Superviser la mise en place d'un cadre de gouvernance pour surveiller et évaluer les progrès en matière de cybersécurité.
- A1T1C3 : Mettre en place et coordonner des comités ou instances de pilotage pour optimiser les indicateurs de performance en cybersécurité.

Tâche 2 (A1T2) : Identifier et analyser les risques liés à la cybersécurité

- A1T2C1 : Utiliser des méthodologies reconnues, telles qu'EBIOS ou ISO 27005, pour réaliser des analyses de risques.
- A1T2C2 : Évaluer les menaces spécifiques à l'organisation et leurs impacts potentiels sur les systèmes d'information.
- A1T2C3 : Rédiger des rapports d'analyse incluant des recommandations opérationnelles pour atténuer les risques.

Tâche 3 (A1T3) : Superviser la mise en œuvre de la gestion des risques

- A1T3C1 : Gérer les risques en coordination avec les équipes techniques.
- A1T3C2 : Piloter des audits internes ou externes pour évaluer la conformité et l'efficacité des mesures.
- A1T3C3 : Implémenter des mesures correctives et réactives adaptées.
- A1T3C4 : Maintenir une veille proactive sur les menaces émergentes, les évolutions technologiques et réglementaires.

Tâche 4 (A1T4) : Gérer une crise de cybersécurité

- A1T4C1 : Coordonner une cellule de crise en définissant des rôles, responsabilités et plans d'action pour limiter les impacts d'un incident de cybersécurité.
- A1T4C2 : Mettre en œuvre et suivre un plan de gestion de crise cyber incluant la communication interne et externe (communication de crise).
- A1T4C3 : Analyser l'incident post-crise afin d'identifier les failles, les causes racines et proposer des améliorations pour renforcer la résilience.
- A1T4C4 : Animer et coordonner des exercices de gestion de crise pour tester la capacité des équipes à réagir face à des incidents de cybersécurité.

Modalités de contrôle des connaissances

Évaluation initiale / Session principale - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
Contrôle Continu	Contrôle Continu		1			

Seconde chance / Session de rattrapage - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
Epreuve terminale	Oral	30		1		